La protection des libertés fondamentales face au développement d'internet

1)Le droit à la protection de la vie privée

L'utilisation de moyens de surveillance et d'interceptions de communications de plus en plus envahissants, le recours à des techniques de détermination et de définition de profils et à la technologie d'identification de paramètres biométriques, le développement de technologies de communication avec des capacités de surveillance intégrées, la collecte de données génétiques utilisées à mauvais escient, les tests génétiques, l'intrusion croissante dans la vie privée sur les lieux de travail et l'affaiblissement des systèmes de protection de données suscitent de graves préoccupations quant à la protection du droit à la vie privée.

De nouveaux moyens doivent être mis en place dans le but de protéger ce droit reconnu à l'article 12 de la DUDH. Ainsi, le droit à connaître les données personnelles détenues par des institutions publiques et privées doit être assuré, de même que la possibilité de les supprimer lorsque leur détention n'est pas indispensable. Le développement, le transfert et l'utilisation de la technologie permettant une invasion illégale de la vie privée, doivent être contrôlés et réduits.

Le respect total de la liberté d'expression et d'information par les acteurs étatiques et privés est une condition préalable indispensable à la construction d'une société d'information et de communication libre et sans exclusion. Les technologies de l'information et de la communication ne doivent pas être utilisées pour limiter cette liberté fondamentale. Il ne doit pas y avoir de censure, de contrôles arbitraires ou de contrainte exercés sur les participants au processus d'information, par rapport au contenu de l'information, sa transmission et sa dissémination. Le pluralisme des sources d'informations et des médias doit être protégé et encouragé.

En application de l'article 19 de la DUDH, toute restriction à la liberté d'expression et d'information doit poursuivre un objectif légitime, au regard du droit international, doit être prescrit par la loi, doit rester strictement proportionnel à un tel objectif et doit être indispensable à une société démocratique pour assurer le respect des droits ou de la réputation des autres, la protection de la sécurité nationale, de l'ordre public, de la santé publique ou de la moralité. Les législations sur la sécurité nationale en vue de combattre le terrorisme, doivent respecter les normes de liberté d'expression et d'information et doivent être soumises à un examen judiciaire et à une analyse internationale approfondie.

Définition :
Le droit international des droits de l'Homme peut concourir à une utilisation éthique d'Internet de part ses valeurs universellement reconnues :
- d'une part en rappelant quelles sont les libertés issues des droits de l'Homme dont disposent les utilisateurs d'Internet ;
- d'autre part en identifiant les obligations issues des droits de l'Homme qu'ils doivent respecter sur Internet envers les autres utilisateurs.

1. Les droits des utilisateurs d'Internet

Les utilisateurs d'Internet, ou internautes, sont l'ensemble des individus qui accèdent à ce réseau afin de s'informer, communiquer, créer, diffuser des informations, héberger des sites, fournir des informations, permettre à d'autres d'accéder à l'information, effectuer des recherches. Ce sont toutes ces personnes qui d'une manière ou d'une autre, dans un but personnel ou professionnel, se connectent au réseau internet…

En tant qu'utilisateur d'Internet, je ne renonce pas à mon humanité. Malgré une apparence parfois déshumanisée du fait de l'utilisation de supports informatiques et numériques, les utilisateurs d'Internet demeurent des êtres humains.
Par conséquent, je bénéficie sur Internet comme ailleurs de la protection issue des droits de l'Homme proclamés dans des conventions internationales sans distinction fondée sur mon sexe, ma race, ma couleur, ma langue, ma religion, mes opinions politiques ou tout autres opinions, mon origine nationale ou sociale, mon appartenance à une minorité nationale, ma fortune, ma naissance ou tout autre situation :

- La liberté d'expression, par la parole, l'écrit, l'image
- La liberté de communication
- La liberté d'accès à l'information
- La liberté de la presse
- Liberté de pensée, de conscience et de religion
- Liberté de réunion et d'association
- Le droit à la protection de la personne :le droit au respect de sa vie privée et familiale, de son domicile et de sa correspondance, de son image, de son honneur et de sa réputation
- Le droit à la protection des données à caractère personnel
- Le droit à l'éducation
- Le droit de participer à la vie culturelle

2. les limites aux droits des utilisateurs d'Internet

On dit souvent que la liberté des uns s'arrête là ou commence celle des autres. En effet, toutes les conventions internationales visant à promouvoir et protéger les droits de l'Homme dans le monde rappellent que l'exercice de ces droits est limité.
Le fait de vivre en communauté implique nécessairement de respecter les autres individus, dotés aussi de droits. Il implique aussi de respecter les prérogatives de l'Etat qui a vocation à organiser cette communauté.

Ainsi, en tant qu'utilisateur d'Internet, je dois respecter ces limites:

- le respect des droits et des libertés d'autrui : de manière générale, les autres utilisateurs ont les même droits que moi, et donc la capacité égale à la mienne de les exercer (liberté d'expression, de communication, de religion, etc…), quels que soit leur race, couleur, sexe, religion, origine nationale ou sociale, leur fortune, ou tout autre différence. De même chaque individu doit respecter la vie privée et familiale, le domicile et la correspondance d'autrui, ainsi que sa réputation et son honneur.
Ex : je ne peux diffuser un texte sur Internet qui porterait atteinte à la réputation d'une autre personne.

Toute propagande en faveur de la guerre, toute incitation à la haine raciale, nationale ou religieuse, toute incitation à la discrimination raciale, toute incitation directe et publique à commettre un génocide sont interdites

3.La protection d'intérêts particuliers :

- la protection des enfants : toute forme d'exploitation sexuelle des enfants est illicite. Nul enfant ne doit être soumis à des traitements inhumains ou dégradants. Par conséquent le fait de produire, de diffuser, d'importer, d'exporter, d'offrir, de vendre ou de détenir des matériels pornographiques mettant en scène des enfants est considéré comme un crime
Ex : je ne peux télécharger des images d'enfants s'adonnant à des activités sexuelles sur Internet et les conserver ;

- la protection des auteurs : chaque auteur a le droit de bénéficier des intérêts moraux et matériels découlant de toute production scientifique, littéraire ou artistique
- l'ordre public, la protection de la santé et de la morale, l'intégrité territoriale, la sûreté publique et la prévention du crime : c'est au nom de ces impératifs que l'Etat peut restreindre les libertés des individus sur Internet. Cependant, afin de conserver le caractère démocratique d'une société, ces restrictions ne peuvent être mises en œuvre que sous réserve de certaines conditions, telles que la proportionnalité ou la nécessité.

Ex : un fonctionnaire peut voir sa liberté d'expression réduite au nom du devoir de réserve afin de protéger l'ordre public.

L'internaute doit aussi savoir que dans le cas d'un danger public exceptionnel menaçant l'existence de la nation (troubles internes, guerre civile, conflit international), certaines libertés peuvent être supprimées ou restreintes (liberté d'expression, liberté de la presse…)

2)

Gouvernance de l'internet

La principale interrogation pour les années à venir sera de savoir comment appliquer une loi nationale au Net, qui ne connaît, par nature, aucune frontière. Les auteurs d'un texte mis en ligne peuvent être attaqués en diffamation dans un pays sur la base d'un texte écrit et mis en ligne n'importe où dans le monde. Dans ce contexte, le salut pourrait, et devrait, venir d'une réaction des instances internationales. L'ONU s'est en effet attelée au dossier d'Internet, cherchant des voies nouvelles pour développer le Réseau tout en le régulant. Mais dans un premier temps, il importe de créer un mécanisme de supervision sous l'égide de l'ONU afin d'enquêter sur les violations des droits de l'Homme commises dans le cadre du développement de la société de l'information et proposer les meilleurs moyens d'orienter son développement en faveur de la réalisation des droits de l'Homme.

La rencontre du droit pénal et de l'informatique ne doit pas surprendre. L'ordinateur est un outil fragile et difficilement contrôlable qui peut être assez aisément manipulé. La fragilité de l'outil informatique conduit le législateur à tenter d'assurer la plus grande sécurité, afin d'éviter les fraudes qui prennent des formes diverses : piratage informatique, création de compte bancaire ou d'assuré social purement fictif, contrefaçon, destruction de système par l'introduction de "virus", intrusion dans la vie privée ou atteintes aux mœurs … Il n'est donc pas surprenant que le droit pénal trouve application dans ce domaine pour sanctionner les différents agissements frauduleux portant notamment atteinte aux droits des personnes.

La fraude informatique, c'est-à-dire l'ensemble des agissements répréhensibles relatifs aux systèmes de traitement automatique d'informations, est un concept proteiforme. Cependant, il apparaît que l'on peut opposer les biens informatiques qui sont l'objet de fraudes (sabotage, piratage, destruction de données …) et les biens informatiques qui sont le moyen de la fraude. L'ordinateur sert alors de vecteur à la réalisation de l'infraction et permet de réaliser des atteintes aux droits des personnes.

L'utilisation de l'ordinateur peut donner lieu à des agissements malhonnêtes, dont il importe de savoir s'ils peuvent recevoir une qualification pénale. Il serait vain de faire l'inventaire de toutes les dispositions pénales applicables. En effet, la plupart des comportements incriminés par le Code pénal peuvent être commis par le biais de l'informatique : abus de confiance, escroquerie, faux, détournement, contrefaçon, atteintes à la paix publique … Cependant, des textes spécifiques intégrés aujourd'hui au Code pénal, les articles 226-16 et suivants, ont été

créés pour sanctionner des comportements particuliers relatifs "aux atteintes aux droits de la personne résultant des fichiers ou des traitements informatiques".

L'application des dispositions pénales à ces fraudes informatiques se heurte à une difficulté principale tenant à la preuve. En effet, ces infractions sont très difficiles à découvrir et souvent la connaissance de ces agissements illicites relève du hasard.

L'informatique peut donc être un moyen de fraude aux effets redoutables s'agissant des personnes. Par le biais du traitement informatique de données, de leur sélection, par le jeu de l'interconnexion de fichiers, de véritables agressions aux droits des personnes peuvent être commises et sanctionnées par le droit pénal. Nous constaterons que ces agressions aux droits des personnes peuvent bien sûr exister en dehors de l'informatique - plus particulièrement en ce qui concerne les infractions contre les mœurs, cependant, l'outil informatique facilite largement leur commission et propage leurs effets.

La loi "Informatique et Libertés" en date du 6 janvier 1978, fut ainsi adoptée pour punir ces comportements délictueux et organiser un contrôle par la Commission Nationale de l'Informatique et des Libertés. Cette loi, aujourd'hui intégrée au Code pénal (articles 226-16 et suivants), permet de sanctionner les atteintes aux droits des personnes (I). Mais au-delà de ces dispositions spécifiques, il faut souligner qu'il est nécessaire de recourir aux textes du droit pénal classique - par opposition au droit pénal de l'informatique - pour réprimer d'autres comportements frauduleux qui ont pour support l'ordinateur et dont les manifestations contemporaines les plus marquantes sont les atteintes aux mœurs (II).

I. INFORMATIQUE ET ATTEINTES AUX DROITS DES PERSONNES

Ces atteintes aux droits des personnes peuvent être divisées en deux catégories, au regard des dispositions des articles 226-16 et suivants du Code pénal. Ces textes conduisent à distinguer d'une part, les enregistrements d'informations (A), d'autre part, les divulgations d'informations (B).

A. Les enregistrements d'informations

L'enregistrement d'informations peut principalement donner lieu à la commission de deux infractions : en premier lieu, le délit de création de fichier clandestin, en second lieu, le délit d'enregistrement ou de conservation illicite d'informations nominatives.

1. La création de fichiers clandestins

Le fait, y compris par négligence, de procéder ou de faire procéder à des traitements automatisés d'informations nominatives, sans qu'aient été respectées les formalités préalables à leur mise en œuvre prévues par la loi, est sanctionné pénalement par des peines de trois ans d'emprisonnement et 300000 Francs d'amende. Les agissements qui sont visés par cette disposition, sont relatifs à la création de fichiers clandestins. Ces fichiers sont clandestins lorsqu'ils sont réalisés sans information ou déclaration préalable auprès de la CNIL, comme l'impose la loi.

2. L'enregistrement ou la conservation illicite d'informations nominatives

Trois articles du Code pénal sanctionnent ces agissements frauduleux (art. 226-18 à 20). Dans les trois hypothèses, le législateur a voulu sanctionner le fait d'obtenir frauduleusement des informations ou de les conserver frauduleusement. Dans les deux cas, la notion de fraude ets déterminante. Ces infractions recouvrent des comportements multiples, par exemple :

> le fait d'obtenir des informations de manière déloyale pour les collecter, par exemple par le biais de questionnaires téléphoniques apparemment anodins, ou de prétendus sondages …

le fait de procéder à une collecte interdite d'informations, eu égard à la nature de celles-ci. L'infraction sera constituée lorsque, en l'absence d'accord express de l'intéressé, des informations auront été obtenues, faisant apparaître les origines raciales, les opinions politiques ou religieuses, les mœurs d'une personne ou des infractions qu'elle aurait pu commettre ou dont elle aurait connaissance.

le fait de conserver en mémoire des informations nominatives, au-delà de la durée prévue dans la déclaration initiale à la CNIL.

B. La divulgation d'informations

Deux délits sont incriminés par le Code pénal en ce qui concerne cette divulgation : d'une part, le manquement à la sécurité des personnes, d'autre part, la divulgation illicite d'informations nominatives.

1. Le manquement à la sécurité

Le législateur sanctionne dans l'article 226-17 du Code pénal, le fait de ne pas prendre toutes les mesures utiles pour préserver la sécurité des informations nominatives enregistrées, pour empêcher qu'elles ne soient déformées, endommagées ou communiquées à des tires non autorisés. Cela ne signifie pas qu'il soit imposé une obligation absolue de sécurité, la loi n'impose pas une obligation de résultat, mais le détenteur de ces informations doit accomplir toutes les diligences utiles à la préservation de ces informations.

2. La divulgation interdite d'informations nominatives

Cette disposition (article 226-22 du Code pénal) ressemble étrangement aux textes du Code pénal sanctionnant la violation du secret professionnel. Trois conditions doivent être réunies pour que l'infraction soit constituée :

Les informations divulguées doivent être de nature à porter atteinte à la considération de la personne ou à l'intimité de sa vie privée. Nous pouvons citer à titre d'exemple, la communication de numéros de téléphone ou de renseignements privés. Il appartiendra au juge d'apprécier la portée de l'information divulguée.

La divulgation doit avoir été faite sans l'autorisation de l'intéressé, ce qui sera généralement le cas, dans la mesure où cela porte atteinte à sa vie privée.

La divulgation doit être faite à des personnes non qualifiées pour la recevoir. Ne sont pas qualifiées les personnes qui n'ont pas été visées dans la déclaration préalable faite à la CNIL qui déterminait qui pouvaient être les destinataires des informations enregistrées.

Nous avons envisagé les infractions principales constitutives d'atteintes aux droits des personnes au sens du droit pénal de l'informatique. Mais, un domaine qui connaît un essor inquiétant donne lieu à la commission de multiples infractions dont la sanction est particulièrement difficile à mettre en œuvre, celui des atteintes aux mœurs.

II. INFORMATIQUE ET ATTEINTES AUX MOEURS

Les atteintes aux mœurs réalisées par le biais de l'informatique ou de la télématique se développent considérablement, la presse s'en fait presque quotidiennement l'écho. Après quelques incertitudes, le droit pénal parvient à encadrer et à sanctionner les infractions commises par la voie du Minitel (A), mais en ce qui concerne les agissements illicites réalisés sur Internet, la législation pénale connaît d'importantes difficultés d'application (B).

A. Les infractions commises sur Minitel

Concernant les atteintes aux mœurs, ce sont essentiellement les messageries dites "roses" qui ont donné lieu à des poursuites pénales et à des sanctions. La question des messageries roses

suscite une double interrogation en matière pénale : en premier lieu, il s'agit de savoir dans quelle mesure une infraction est commise, en second lieu, il faut déterminer qui est le responsable des agissements délictueux.

1. Pour être constituée, l'infraction implique que soit attirée l'attention sur une occasion de débauche de manière publique (art. 227-24 du Code pénal)

La question est donc de savoir si, par l'utilisation du Minitel, cette condition de publicité est remplie. Nombreuses ont été les personnes poursuivies qui ont soutenu que la consultation de ces messageries relevait du domaine de la correspondance privée, échappant ainsi aux prévisions du droit pénal.

La correspondance privée étant couverte par le secret de la correspondance, elle ne peut donner lieu à la commission d'agissements pénalement sanctionnés. Cette argumentation a été rejetée par la jurisprudence qui a distingué deux phases au sein de la communication télématique. La première phase consiste à effectuer le branchement de l'usager sur la messagerie désirée. Cette phase est accessible à toute personne qui se connecte sur la messagerie. Il ne s'agit donc en aucun cas de communication privée. La seconde phase débute au moment où les correspondants entrent en relation. Tout ce qui s'affiche sur l'écran est alors inaccessible aux autres usagers. Une correspondance télématique privée s'établit, échappant alors à la sanction pénale. Donc, seule la partie initiale de la communication est susceptible de tomber sous le coup de la sanction pénale.

2. La recherche d'un responsable pénal

Cette question soulève bien des difficultés. Qui est l'auteur de l'infraction ? des complicités peuvent-elles être retenues ?

Après de multiples hésitations, la jurisprudence la plus récente de la Chambre Criminelle de la Cour de Cassation considère que l'auteur principal de l'infraction ne peut être que le responsable de l'exploitation de la messagerie rose, l'usager du Minitel pouvant, selon les cas, être poursuivi en tant que coauteur, mais le plus souvent comme complice. Cette jurisprudence est cependant susceptible d'évoluer face à la résistance des juridictions du fond, qui considèrent plutôt que le responsable est l'utilisateur qui a effectué la connexion télématique, le serveur n'étant que le complice par aide ou assistance.

B. La criminalité sur Internet

En facilitant les communications et la diffusion d'informations à l'échelle planétaire, Internet favorise la commission d'infractions et apparaît comme le vecteur d'une nouvelle forme de délinquance contre laquelle l'application de notre droit pénal bute pour identifier les auteurs, eu égard à cette dimension internationale. Les agissements délictueux sont innombrables : diffusion d'images pornographiques (la brigade norvégienne de lutte contre la criminalité informatique a identifié 6000 sites pornographiques), messages racistes, reproduction d'une œuvre sans l'accord de son auteur, diffamations, injures, atteintes à la vie privée …

La difficulté tient à ce qu'Internet nous confronte à l'hétérogénéité des systèmes juridiques à l'échelon de la planète, ce qui est répréhensible en France ne l'est pas nécessairement ailleurs. Cela entrave la coopération judiciaire internationale, sans laquelle une répression efficace semble impossible.

Une autre difficulté majeure tient à la preuve des infractions commises. La preuve de la connexion sur un site est extrêmement difficile à établir. Il est intéressant de constater que les autorités policières françaises ont mis au point des formations spécifiques des personnels de la police face à cette nouvelle forme de délinquance. Un des moyens de preuve des infractions commises consistant à saisir le disque dur des ordinateurs et à l'analyser, des compétences techniques de haut niveau sont désormais indispensables.

Face à cette nouvelle délinquance et aux difficultés qu'elle engendre, le droit pénal offre cependant des recours, à condition de pouvoir déterminer le responsable. En effet, les dispositions relatives à la protection de l'individu et aux contrôles des données nominatives doivent également être respectées et l'on retrouve ici les règles que nous évoquions précédemment.

En conclusion, il faut souligner que la CNIL a remis le 4 juillet 1997 au Président de la République un rapport dans lequel elle fait le point sur la protection des données personnelles et insiste sur le nécessité d'assurer le meilleur encadrement des traces informatiques. Son objectif étant de mettre en place une politique efficace de sensibilisation au respect des droits de la personne, tels que définis par la loi Informatique et Libertés.

3) Deux adolescents ont été condamnés par la Justice néerlandaise pour violences et "vol virtuel".

La scène se passe en septembre 2007 aux Pays-Bas, lorsque ces derniers poussent - sous la menace d'un couteau - un camarade de classe à leur donner deux objets acheter sur l'univers virtuel Runescape. Les parents du jeune garçon ont porté plainte, invitant le juge à considérer ces objets comme "réels et tangibles", dans la mesure où ils ont été acheté avec de l'argent réel.

Les juges ont donné gain de cause au plaignant, condamnant les deux adolescents néerlandais à des peines d'intérêt général.

Cette jurisprudence pourrait avoir des conséquences aux Pays-Bas. Un procès similaire devrait s'ouvrir prochainement à Amsterdam, après que cinq jeunes aient volé pour 4000 euros de mobilier virtuel sur le jeu Habbo Hotel, en demandant à des utilisateurs leur mot de passe par des méthodes de pharming.

Infractions sur internet : les nouvelles règles du jeu

La loi du 5 mars 2007 relative à la prévention de la délinquance comporte un volet important consacré aux infractions commises sur internet. Ce nouveau texte, à travers des dispositions propres aux nouvelles technologies, complète le droit pénal qui, jusqu'ici, considérait le recours aux Tic comme une circonstance aggravante des délits (traite des êtres humains, proxénétisme...).

Première disposition importante : le parquet peut désormais saisir le juge des référés pour qu'il ordonne la fermeture d'un site internet. Sont visés les sites diffusant des messages encourageant les crimes et délits, les sites faisant l'apologie des crimes de guerre et des crimes contre l'humanité, ou encore ceux favorisant les actes de terrorisme, la discrimination, la haine, la violence ethnique, religieuse ou sexuelle.

Les moyens de la police judiciaire pour faciliter la collecte des preuves de délits commis sur des mineurs via internet et identifier leurs auteurs sont renforcés. Sur le modèle des opérations d'infiltration, autorisées par la loi du 9 mars 2004 pour lutter contre le crime organisé, le code de procédure pénale permet désormais aux agents de police judiciaire, spécialement habilités, de participer aux échanges électroniques sous un pseudonyme, d'entrer en contact avec des auteurs potentiels d'infraction et d'extraire et conserver des contenus illicites. La police

judiciaire devra néanmoins veiller à ne pas inciter les internautes à commettre des infractions, sous peine de nullité de la procédure.

Lutter contre les sites illicites de jeux en ligne

La loi responsabilise également les hébergeurs et fournisseurs d'accès. Ceux-ci sont tenus de participer à la lutte contre la diffusion de messages violents, pornographiques ou de nature à porter gravement atteinte à la dignité humaine. Les prestataires techniques ont ainsi l'obligation de mettre en place un dispositif accessible et visible permettant que leur soient signalées ces infractions.

Enfin, le législateur a introduit des dispositions destinées à faire barrage aux sites de jeux en ligne illicites : les hébergeurs et les fournisseurs d'accès sont tenus de mettre à la disposition de leurs abonnés un signalement de ces sites

4)

La Commission Nationale de l'Informatique et des Libertés (CNIL) a été instituée par relative à l'informatique, aux fichiers et aux libertés qui la qualifie d'autorité administrative indépendante.

La CNIL c'est :

Un collège pluraliste de :

- 4 parlementaires (2 députés, 2 sénateurs),
- 2 membres du Conseil économique et social,
- 6 représentants des hautes juridictions (2 conseillers d'État, 2 conseillers à la Cour de cassation, 2 conseillers à la Cour des comptes),
- 5 personnalités qualifiées désignées par le Président de l'Assemblée nationale (1 personnalité), par le Président du Sénat (1 personnalité), par le conseil des ministres (3 personnalités).

Le mandat de ses membres est de 5 ans ou, pour les parlementaires, d'une durée égale à leur mandat électif.

Pour conduire leurs missions, les membres de la CNIL s'appuient sur .

Une autorité indépendante :

12 des 17 membres sont élus par les assemblées ou les juridictions auxquelles ils appartiennent.

La CNIL élit son Président parmi ses membres ; elle ne reçoit d'instruction d'aucune autorité ; les ministres, autorités publiques, dirigeants d'entreprises, publiques ou privées, ne peuvent s'opposer à l'action de la CNIL pour quelque motif que ce soit et doivent prendre toutes mesures utiles afin de faciliter sa tâche.

Le Président de la CNIL recrute librement ses collaborateurs.

Une autorité administrative :

- Le budget de la CNIL est imputé sur le budget de l'État.
- Les agents de la CNIL sont des agents contractuels de l'État.
- Les décisions de la CNIL peuvent faire l'objet de recours devant la juridiction administrative.

Face aux dangers que l'informatique peut faire peser sur les libertés, la CNIL a pour mission essentielle de protéger la vie privée et les libertés individuelles ou publiques. Elle est chargée de veiller au respect de la loi "Informatique et Libertés" qui lui confie 5 missions principales :

Informer

La CNIL informe les personnes de leurs droits et obligations, et propose au gouvernement les mesures législatives ou réglementaires de nature à adapter la protection des libertés et de la vie privée à l'évolution des techniques. L'avis de la CNIL doit d'ailleurs être sollicité avant toute transmission au Parlement d'un projet de loi créant un traitement automatisé de données nominatives.

Garantir le droit d'accès.

La CNIL veille à ce que les modalités de mise en oeuvre du droit d'accès aux données contenues dans les traitements n'entravent pas le libre exercice de ce droit. Elle exerce, pour le compte des citoyens qui le souhaitent, l'accès aux fichiers intéressant la sûreté de l'État, la défense et la sécurité publique, notamment ceux des Renseignements généraux.

Recenser les fichiers.

Les traitements de données à “risques” sont soumis à autorisation de la CNIL. Elle donne un avis sur les traitements publics utilisant le numéro national d'identification des personnes. Elle reçoit les déclarations des autres traitements. Le non-respect de ces formalités par les responsables de fichiers est passible de sanctions administratives ou pénales. La CNIL tient à la disposition du public le "fichier des fichiers", c'est-à-dire la liste des traitements déclarés et leurs principales caractéristiques.

Contrôler

La CNIL vérifie que la loi est respectée en contrôlant les applications informatiques. La Commission use de ses pouvoirs de vérification et d'investigation pour instruire les plaintes, pour disposer d'une meilleure connaissance de certains fichiers, pour mieux apprécier les conséquences du recours à l'informatique dans certains secteurs, pour assurer un suivi de ses délibérations. La CNIL surveille par ailleurs la sécurité des systèmes d'information en s'assurant que toutes les précautions sont prises pour empêcher que les données ne soient déformées ou communiquées à des personnes non-autorisées.

Sanctionner

La CNIL peut prononcer diverses sanctions graduées : avertissement, mise en demeure, sanctions pécuniaires pouvant atteindre 300 000 €, injonction de cesser le traitement. Enfin, le Président peut demander par référé à la juridiction compétente d'ordonner toute mesure de sécurité nécessaire. Il peut, au nom de la Commission, dénoncer au Procureur de la République les violations de la loi.

Réglementer

La CNIL établit des normes simplifiées, afin que les traitements les plus courants et les moins dangereux pour les libertés fassent l'objet de formalités allégées.

Elle peut aussi décider de dispenser de toute déclaration des catégories de traitement sans risques.